International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 6, Issue 1, Feb 2016, 43-52

TRANS STELLAR
•Journal Publications •Research Consultancy

Original Article

AN EVALUATION ON MODERN SPATIAL DOMAIN IMAGE STEGANOGRAPHIC ALGORITHMS

S. DEEPA[1] & R. UMARANI[2]

[1]*Assistant Professor, Department of Computer Science, Government Arts College, Dharmapuri, Tamil Nadu, India*

[2]*Associate Professor, Department of Computer Science, Sri Sarada College for Women, Salem, Tamil Nadu, India*

ABSTRACT

The classical spatial domain image steganography techniques of previous decades generally used some of the simple LSB insertion techniques for hiding information in a cover image. But the modern spatial domain image steganography techniques uses the state of the art methods for pixel selection to hide the information in appropriate pixels to reduce the risk of visual and statistical attacks. The modern techniques made the embedding changes to selected parts of the cover image such as textures or noisy regions, while avoiding smooth regions or clean edges to make it difficult for an attacking method to guess the presence of steganography in the image. The only task is the design of the distortion function. This paper consists of five state of art content-adaptive steganographic techniques of this decade for the evaluation. The methods are Spatial Version of Universal Wavelet Relative Distortion (S_UNIWARD), Wavelet Obtained Weights (WOW) Algorithm, Multivariate Gaussian (MG) Model, Multivariate Generalized Gaussian (MVG or MVGG) Model, and Minimizing the Power of Optimal Detector (MiPOD) Algorithm. By using suitable metrics the performance of the five different steganography methods are evaluated.

KEYWORDS: S_UNIWARD, WOW, MG, MVGG, MiPOD

Received: Dec 29, 2015; **Accepted:** Jan 04, 2016; **Published:** Jan 21, 2016; **Paper Id.:** IJCSEITRFEB20166

INTRODUCTION

- ***Steganography***

"Steganography is the art and science of communicating in a way which hides the existence of the communication. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present". That means steganography technique embed the secret message into a cover media that can be image, text, audio or video in such a way that attackers don't have any idea about the original message that the media may contain and also which algorithm is used to embed or retrieve it. In a steganography system there are two entities i.e. cover image and message. The hidden message is called the embedded message. At transmitter side these two are combined using one of the algorithms, thus presence of secret message cannot be recognized. This combination thus obtained is termed as stego-message or stego-image. Data type of cover message and stego message must be of the same; however the data type of embedded message may be different. At receiver side reverse steganography algorithm is used to extract the embedded message or secret message.

THE ALGORITHMS UNDER EVALUATION

- **Universal Wavelet Relative Distortion (UNIWARD) and Spatial Version of UNIWARD (S_UNIWARD)**

Universal distortion design also called universal wavelet relative distortion (UNIWARD) is a stego method which is independent of the embedding domain [1]. The embedding distortion is computed as a sum of relative changes of wavelet coefficients with respect to cover image. The distortion function is constructed by using the outputs of a directional filter bank where textured/noisy areas of a given image can be quantified.

The embedding method that uses the additive approximation of UNIWARD for the spatial domain is called S_UNIWARD. In this algorithm, the distortion between the cover and stego image is computed as a sum of relative changes of wavelet coefficients representing both images.

- **Wavelet Obtained Weights (WOW) Algorithm**

WOW defines additive steganographic distortion in the spatial domain. Additive in the sense the distortion does not consider the effects of individual embedding changes influencing each other [2]. A bank of directional filters is employed to obtain the directional residuals, which assess the content around each pixel along multiple directions. The changes in the residuals caused by embedding are measured and aggregated forcing the embedding cost of a pixel to be high where the content is predictable in at least one direction (smooth areas and along edges) and low where the local content is unpredictable in any direction (e.g., in textured or noisy areas).

If the residual values are large for a pixel in all directions, it means that the local content at that pixel is not smooth in any direction. So the embedding prefers changing large values of directional residuals, where the textures and edges are, and preserve the small values, where the content is predictable.

- **Multivariate Gaussian (MG) Model**

In MG model the embedding change probabilities are derived to minimize the Kullback-Leibler (KL) divergence between the cover and stego objects [3]. It models the cover pixels as a sequence of independent Gaussian random variables with n equal variance. The non-stationarity of this model can capture the varying content in images. The Least Significant Bit Matching (LSBM) is used as the embedding operation. The method of Lagrange multipliers is used to derive the optimal embedding change probabilities for a given payload and image. The embedding cost depends on the payload. This is because the KL divergence is minimized in a multivariate Gaussian model rather than an embedding cost fixed for each pixel in the beginning. So the distortion profile for this embedding algorithm depends on the payload. MG uses ternary embedding and preserves some adaptability.

- **Multivariate Generalized Gaussian (MVG or MVGG) Model**

MVGG adopts a strategy of embedding larger payload in highly textured areas [4]. The embedding scheme is designed to minimize the power of the most powerful detector within a chosen cover model. i.e., the distortion is related to statistical detectability. The pixel cost is derived directly from the impact of making an embedding change on the statistical detectability for the chosen cover model.

Generalized Gaussian allows embedding changes with amplitude larger than 1 to embed a larger payload in pixels from textured areas. Prior to embedding it estimates the parameters of the cover model and the local variance at each cover pixel. Then, the costs (the probabilities with which each pixel should be changed by a certain amount or the change rates)

are computed by solving a pair of non-linear algebraic equations in order to minimize the KL divergence between the cover and stego images and minimizing the power of an optimal statistical test. Automatically the cost naturally depends on the payload.

- **Minimizing the Power of Optimal Detector (MiPOD) [5]**

MiPOD pursue an alternative approach based on a locally-estimated multivariate Gaussian cover image model that is sufficiently simple to derive a closed-form expression for the power of the most powerful detector of content-adaptive LSB matching but, at the same time, complex enough to capture the non-stationary character of natural images. It was shown that when the cover model estimator is properly chosen, state-of-the-art performance can be obtained. The closed-form expression for detectability within the chosen model is used to obtain new fundamental insight regarding the performance limits of empirical steganalysis detectors built as classifiers. In particular, it considers a novel detectability-limited sender and estimates the secure payload of individual images.

IMPLEMENTATION AND EVALUATION

- **Message Insertion in Spatial Domain**

  The following is the generalized form of message insertion process in a typical spatial steganography method.

  - **Inputs:** Bits Per Pixel and Payload.
  - Estimate the number of pixels ‘N’ needed for spatial domain insertion with respect to the allowed Bits Per Pixel and message Payload Size.
  - With respect to the algorithm, select ‘N’ pixels in specific regions of the cover image. (such as textures or noisy regions, while avoiding smooth regions or clean edges to make it difficult for an attacking method to guess the presence of steganography in the image).
  - Hide the bits of Message Payload at that selected ‘N’ pixels in a specific predefined order using insertion technique of that algorithm.
  - Store the Stego Image.

- **Message Extraction from Spatial Domain**

  The following is the generalized form of message extraction process in a typical spatial steganography method.

  - **Inputs:** Bits Per Pixel and Expected Payload Size.
  - Estimate the number of pixels ‘N’ with respect to the Bits Per Pixel and message Payload Size from which the message payload can be extracted.
  - With respect to the algorithm, select the ‘N’ pixels in specific regions of the stego image.
  - Retrieve the bits of Message Payload from that selected ‘N’ pixels in a specific predefined order using extraction technique of that algorithm.
  - Save the extracted Message Payload.

  This evaluation needs only the message insertion part of the algorithm.

- **The Evaluation Model**

The following diagram shows the outline of the proposed evaluation strategy:

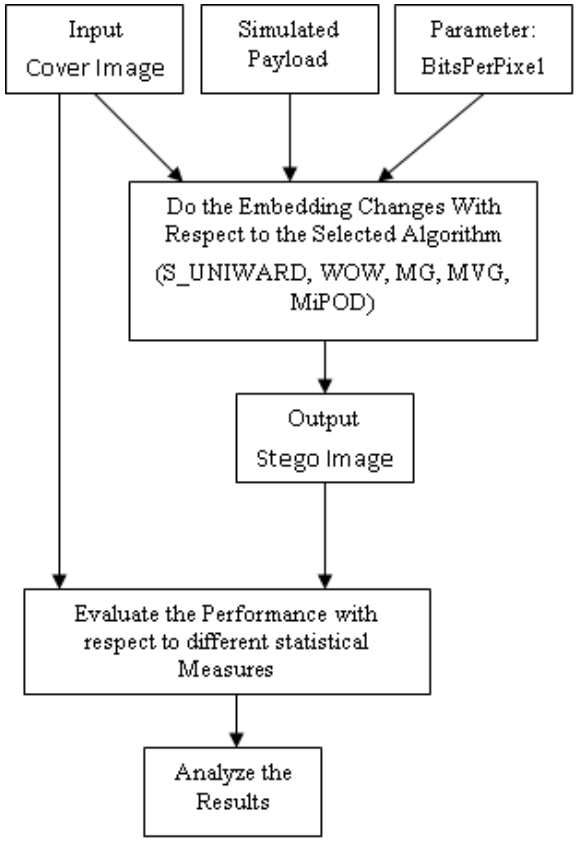


Figure 1: The Implemented System

THE RESULTS AND DISCUSSIONS

- **The Image Database Used**

The Images used for this evaluation were originally taken from the BOWS Image Dataset. BOWS (Break Our Watermarking System) is a Contest organized within the activity of the Watermarking Virtual Laboratory (Wavila) of the European Network of Excellence ECRYPT. In fact, the original dataset contains 10,000 images. This paper uses few cover images from BOWS database that were previously used in another work named “Gibbs Construction in Steganography[6]”.

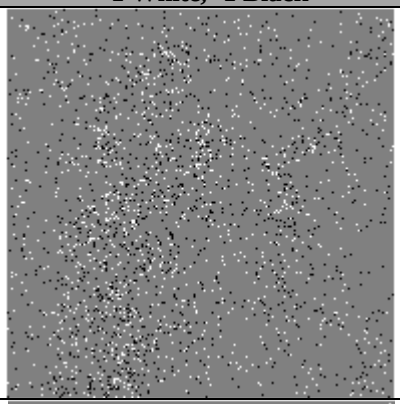
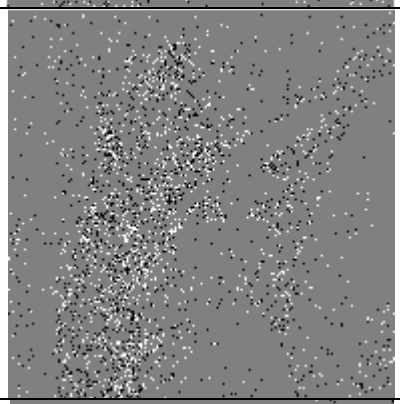
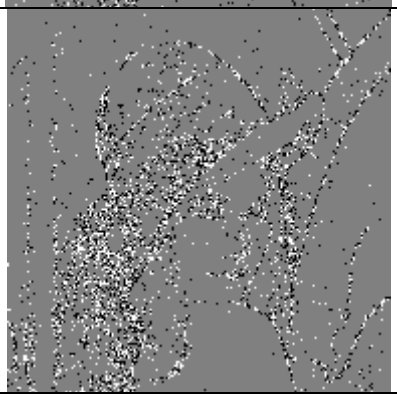
- **A Sample Result with Lenna Image**

As a general convention Lenna image is used to demonstrate the performance of the different algorithms at the level of hiding at 0.40 bits per pixel.

The Original Input Image of size 512x512

Figure 2: A Sample Cover Image

- **The Output Result with Different Steganograpy Algorithms (at 0.04 bits per pixel)**

The Algorithm	Stego Image	Embedding Changes +1 White, -1 Black
S_UNIWARD Time Taken for Embedding: 4.00 sec, Change Rate: 0.0682, PSNR: 59.8251		
WOW Time Taken for Embedding: 2.48 sec, Change Rate: 0.0781, PSNR: 59.2358		
MG Time Taken for Embedding: 6.74 sec, Change Rate: 0.1120, PSNR: 57.6732		

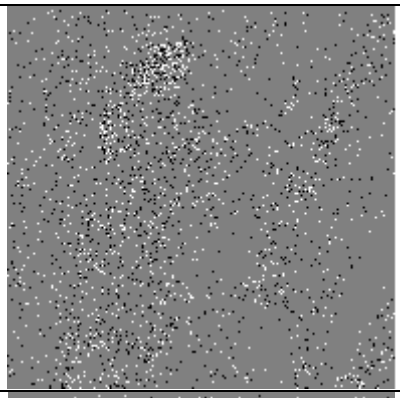
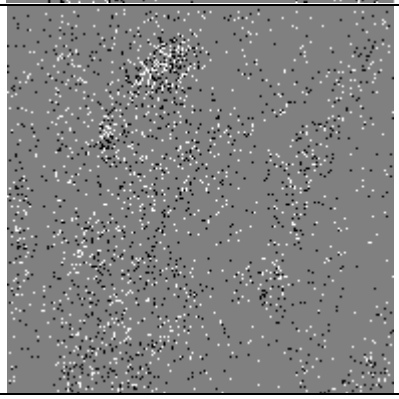
MiPOD Time Taken for Embedding: 6.32 sec, Change Rate: 0.0706, PSNR: 59.6771		
MVG Time Taken for Embedding: 26.03 sec, Change Rate: 0.0697, PSNR: 59.6483		

Figure 3: The Performance with Respect to Different bpp. for Visual Analysis

- **The Average Results with respect to Different Bits per Pixel**

This analysis uses 29 cover images from BOWS database that were previously used in another work named "Gibbs Construction in Steganography". The results in the following section were prepared from the average of 29 values. The tables in the annexure section presents the actual average values from which these graphs are prepared.

The following graph shows the Average Performance of Different steganography algorithms with respect to PSNR at different bpp level of hiding. As shown in the graph, the quality of the stego image decreases with respect to the increase of level of hiding. The S-UNIWARD algorithm provided highest performance in terms of PSNR. In this case, WOW provides medium average performance.

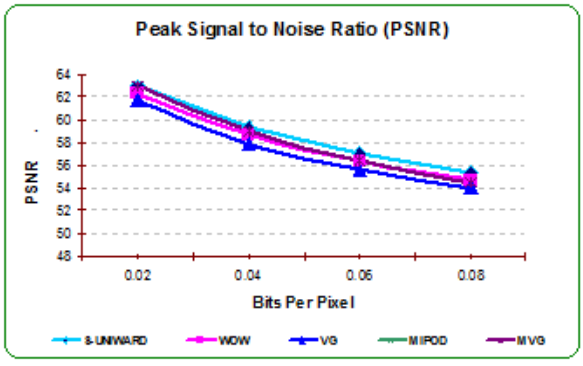


Figure 4: Performance in Terms of PSNR

The following graph shows the Average Performance of Different steganography algorithms with respect to Change Rate at different bpp level of hiding. As shown in the graph, the change rate increased with respect to the increase

of level of hiding. The S-UNIWARD algorithm provided good performance in terms of change rate. The lower change rate of S-UNIWARD signifies that the detection of this stego is some what difficult by a Steganalysis. MVG also provides low change rate. In this case, WOW provides medium performance.

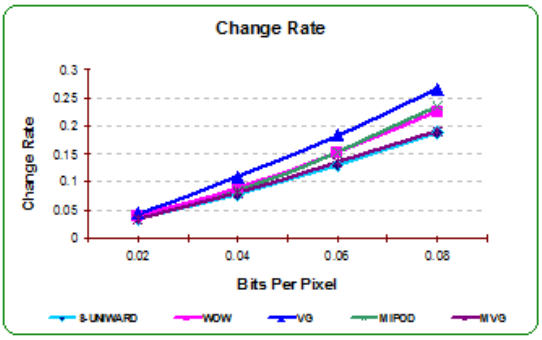


Figure 5: Performance in Terms of Change Rate

The following graph shows the Average Performance of Different steganography algorithms with respect to CPU time at different bpp level of hiding. As shown in the graph, the time consumed by the algorithm increases with respect to the increase of level of hiding. The WOW and S-UNIWARD algorithm provided good performance in terms of CPU time.

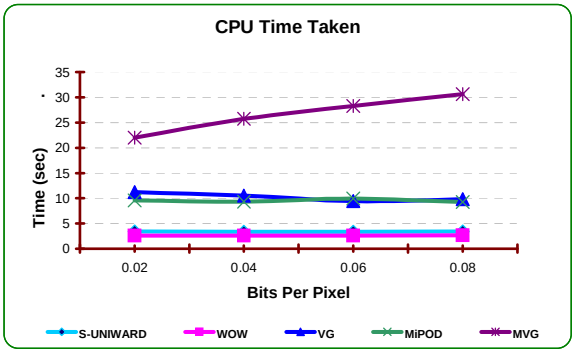


Figure 8: Performance in Terms of CPU Time

The following graph shows the Average Performance of Different steganography algorithms with respect to MSE at different bpp level of hiding. As shown in the graph, the mean square error increases with respect to the increase of level of hiding. The S-UNIWARD algorithm provided highest performance in terms of MSE.

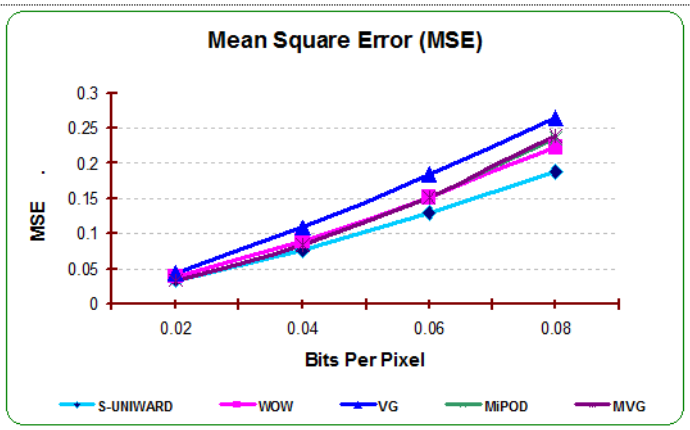


Figure 7: Performance in Terms of MSE

The following graph shows the Average Performance of Different steganography algorithms with respect to MAE at different bpp level of hiding. As shown in the graph, the mean average error increases with respect to the increase of level of hiding. The S-UNIWARD algorithm provided highest performance in terms of MAE.

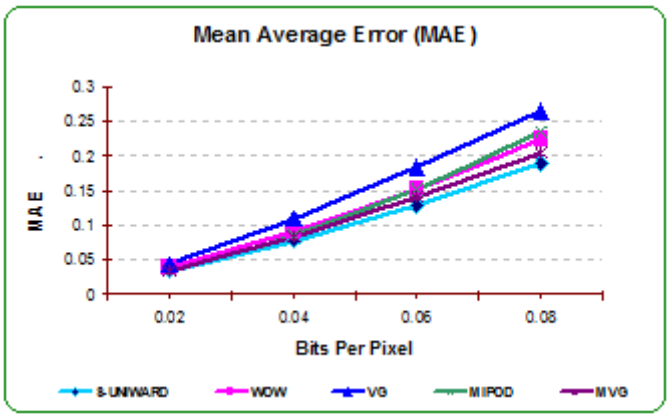


Figure 8: Performance in Terms of MAE

The following graph shows the Average Performance of Different steganography algorithms with respect to RMSE at different bpp level of hiding. As shown in the graph, the root mean square error increases with respect to the increase of level of hiding. The S-UNIWARD algorithm provided highest performance in terms of RMSE.

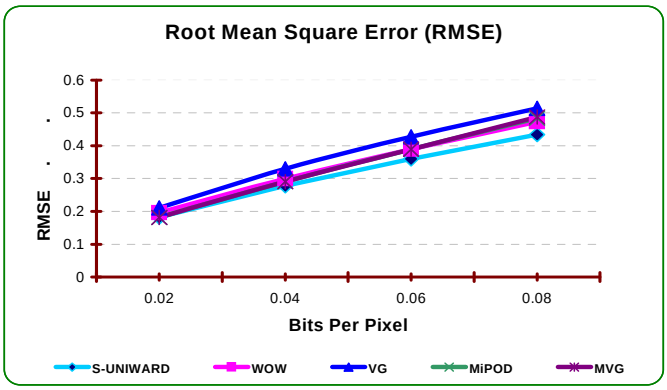


Figure 9: Performance in Terms of RMSE

CONCLUSIONS

This paper successfully implements a Matlab framework for evaluating different state of the art steganography algorithms. Steganography on images are done using five algorithms at different bpp level of hiding. Further, using the cover images and all the different stego images, the performance of the algorithms with respect to different metrics are evaluated.

According to the arrived results, the S-UNIWARD algorithm seems to be providing best performance in terms of most of the considered metrics. Next to that the algorithm WOW performed good. MVG is not considered since it performed very poor in terms of cpu time. In terms of CPU time, S-UNIWARD and WOW performed very good. The time consumption of the algorithm is a very imprtant aspect if the data which is to be hided is huge. Even though MVG performed little bit better than WOW in some cases, WOW is supported because, MVG consumed abnormally higher time than all other algorithms.

The original authors of the algorithms claim that their algorithm will reduce the detection probaility by some means. But according to the observation, if the algorithm claims that it can not be easily detected by steganalyser, then its change rate also becomes low (ex :S-UNIWARD and MVG). Carefuly looking in to the minor differences in results, it states that the performance of the all the five algorithms are some what nearly equal with respect to most of the metrics. If the algorithm becomes secured, then it is able to hide only a little and so the change rate becomes low. So, its clear that WOW provides better performance in between these two extremes.

The challenges between steganography algorithms and steganalysis methods were continuing for the last few decades. Upto now, there is a no winning, fool proof and safe steganography algorithms or steganalysis method. Novel sophisticated steganographic methods will require much novel feature detection methods as well as good feature matching approach for reliable detection. Targeted detection methods may provide reliable results. But there is no reliable method for guessing the stego algorithm for applying a particular targeted detection method. So, the universal blind detection methods are attractive and important research direction because of their flexibility to adapt to any new or unknown steganographic method.

Future works are to address the ways to use the feature sets or feature detection algorithms in the design of a practical steganalysis system. Further to address the application of suitable feature selection and feature reduction techniques to improve the classification performance of a steganalysis system.

ANNEXURE

The Overall Average Performance of Different Steganography algorithms

Table 1: The Average Performance of S-UNIWARD at Different Bits Per Pixel

BPP	CPU Time	MSE	RMSE	MAE	PSNR	Change Rate
0.02	3.42	0.0334	0.1825	0.0334	62.9438	0.0334
0.04	3.37	0.0774	0.2781	0.0774	59.2860	0.0774
0.06	3.38	0.1297	0.3600	0.1297	57.0454	0.1297
0.08	3.42	0.1880	0.4334	0.1880	55.4312	0.1880

Table 2: The Average Performance of WOW at Different Bits Per Pixel

BPP	CPU Time	MSE	RMSE	MAE	PSNR	Change Rate
0.02	2.60	0.0384	0.1956	0.0384	62.3533	0.0384
0.04	2.58	0.0900	0.2995	0.0900	58.6499	0.0900
0.06	2.61	0.1520	0.3893	0.1520	56.3691	0.1520
0.08	2.63	0.2240	0.4727	0.2240	54.6838	0.2240

Table 3: The Average Performance of VG at Different Bits Per Pixel

BPP	CPU Time	MSE	RMSE	MAE	PSNR	Change Rate
0.02	11.21	0.0447	0.2109	0.0446	61.6963	0.0446
0.04	10.53	0.1090	0.3295	0.1090	57.8235	0.1090
0.06	9.43	0.1832	0.4273	0.1831	55.5644	0.1831
0.08	9.81	0.2643	0.5134	0.2642	53.9670	0.2642

Table 4: The Average Performance of MiPOD at Different Bits Per Pixel

BPP	CPU Time	MSE	RMSE	MAE	PSNR	Change Rate
0.02	9.57	0.0332	0.1819	0.0332	62.9781	0.0332

Table 4 Contd.,						
0.04	9.32	0.0845	0.2902	0.0845	58.9299	0.0845
0.06	9.92	0.1521	0.3892	0.1521	56.3805	0.1520
0.08	9.22	0.2350	0.4838	0.2350	54.4911	0.2350

Table 5: The Average Performance of MVG at Different Bits per Pixel

BPP	CPU Time	MSE	RMSE	MAE	PSNR	Change Rate
0.02	22.03	0.0331	0.1818	0.0330	62.9856	0.0330
0.04	25.72	0.0848	0.2906	0.0825	58.9176	0.0814
0.06	28.31	0.1520	0.3890	0.1407	56.3868	0.1351
0.08	30.68	0.2389	0.4874	0.2054	54.4328	0.1886

REFERENCES

1. *V. Holub, J. Fridrich, and T. Denemark, "Universal distortion design for steganography in an arbitrary domain", EURASIP Journal on Information Security, Special Issue on Revised Selected Papers of the 1st ACM IH and MMS Workshop, vol. 2014:1, 2014.*
2. *Holub and J. Fridrich, "Designing steganographic distor- tion using directional filters", in Proc. IEEE WIFS, (Tenerife, Spain), December 2-5, 2012.*
3. *J. Fridrich and J. Kodovsky, "Multivariate Gaussian model for designing additive distortion for steganography", Proc. IEEE, ICASSP, Vancouver, Canada, May 26-31, 2013.*
4. *V. Sedighi, J. Fridrich and R. Cogranne, "Content-Adaptive Pentary Steganography Using the Multivariate Generalized Gaussian Cover Model", Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics 2015, vol. 9409, San Francisco, CA, February 8–12, 2015.*
5. *V. Sedighi, R. Cogranne and J. Fridrich, "Content-Adaptive Steganography by Minimizing Statistical Detectability", IEEE Transactions on Information Forensics and Security.*
6. *http://bows2.ec-lille.fr/*